# ベネッセのサーバ3千台を支えているインフラ担当が語る！
# 本当に効果のある内部不正対策とは

株式会社ベネッセコーポレーション
DIGITAL INNOVATION PARTNERS
インフラソリューション部　インフラサービス2課
高木信剛

# ベネッセグループの事業一覧

**Benesse**
**「よく生きる」**

**誰もが一生、成長できる。**
**自分らしく生きられる世界へ。**
**ベネッセは目指しつづけます。**

| 妊娠・出産、幼児 | 小学生・中学生・高校生 | 学校 | 大学、社会人 | シニア |
|---|---|---|---|---|
| たまひよ | 進研ゼミ | 進研模試 | doda キャンパス | アリア |
| こどもちゃれんじ | 進研ゼミ 個別指導教室 | GTEC | udemy | くらら |
| サンキュ! | 東京個別指導学院 | Classi | STUDY HACKER ENGLISH COMPANY | まどか |
| ベネッセの英語教室 BE studio | 鉄緑会 | ミライシード | | ベネッセのおうちごはん |
| ベネッセの保育園 | 研伸館 | | | ハートページ |
| | ELS | マナビジョン | | 介護求人ナビ |

# 本日お話しすること

**サーバの運用をしている現場視点から、以下の2点について、お話しさせていただきます。**

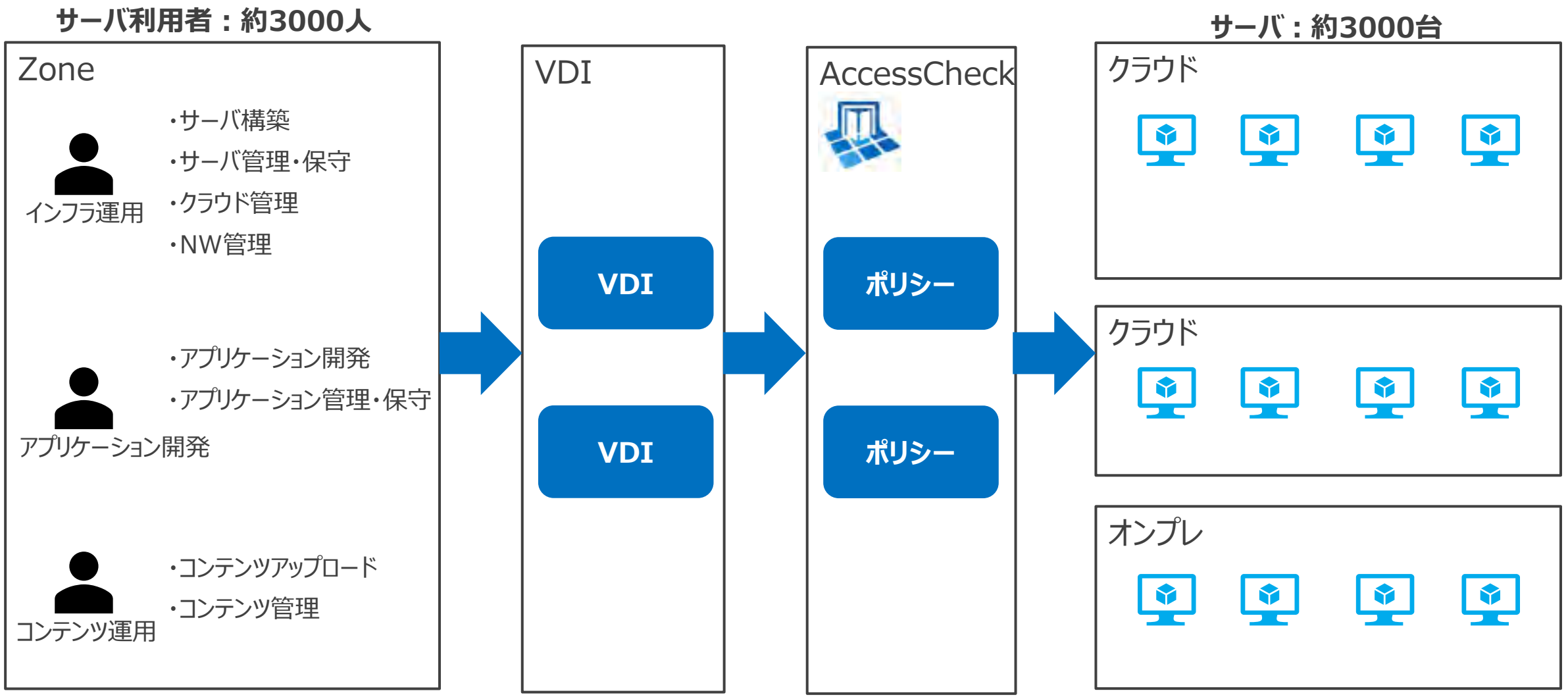
- **サーバ運用に対して、セキュリティ効果のあった対策と改善事例の紹介**
  日々インフラ運用している現場視点から、内部不正の抑止や、セキュリティ意識向上した施策や、その施策の改善事例について紹介させていただきます。

- **「SecureCube Access Check」のさらなる活用**
  特権IDの管理に関しては、長期間の運用や環境の変化に伴い、新たな課題やリスクが発生してきており、現在取り組んでいる「SecureCube Access Check」の機能を活用した新たな特権ID管理方法について共有させていただきます。

# サーバ運用に対して、セキュリティ効果のあった対策と改善事例の紹介

# 環境について

多様な目的で、多様な手段で利用者が、それぞれのサーバにアクセスしている。



# 事例①：操作環境の隔離

個人情報の有無によって、物理的、論理的に隔離が行われ、2重に抑制が効いている

**物理的隔離**


Zone4

サーバ管理

**論理的隔離**

VDI

**個人情報あり VDI**

個人情報ありシステム

**２重の隔離**


Zone2

サーバ管理

VDI

**個人情報なし VDI**

個人情報なしシステム

# 事例①：操作環境の隔離

接続先の環境によって隔離されているので、間違って、個人情報を操作することがない。操作担当者を守るという意味でも、重要な施策だと考えてます。

**Pros**

- 個人情報の完全分離
  個人情報を扱うかどうかで、環境が完全に分離されており、持ち出しに対して、最大の抑止になっている。
- 個人情報に対する意識向上
  個人情報を扱うときに場所とVDIを切り替えることで、重要性を**意識づける**ことが出来る

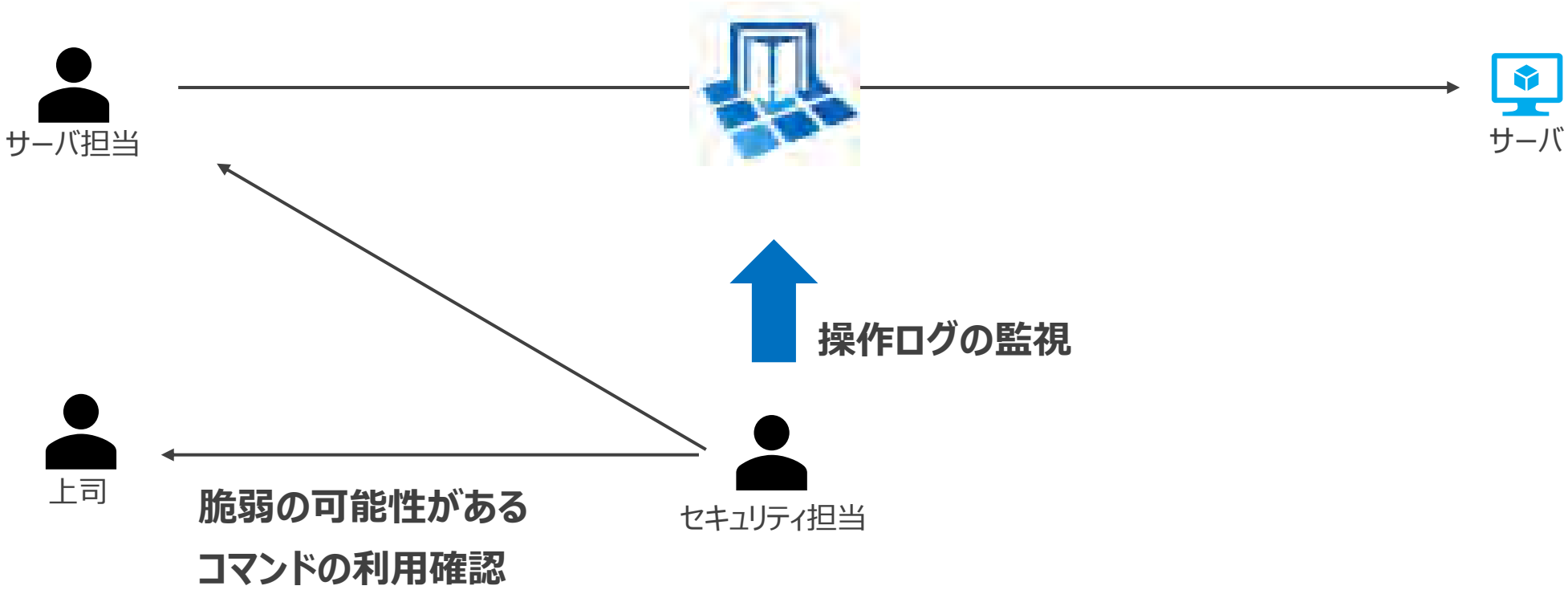
**Cons**

- 維持コスト増
  物理的にZoneを分ける必要があるので、初期投資と維持コストがかかる
- Zone移動の手間
  接続先サーバに合わせて、場所を移動しないといけない

**論理的に分離するだけでも、有効**

# 事例②：操作ログの監視

サーバ操作は必ずAccessCheckを通るようになっており、その操作ログをセキュリティ担当が監視し、システムを脆弱にしてしまったり、不正な行為の可能性のある操作に正当性があるか確認



# 事例②：操作ログの監視

セキュリティ担当からこの確認があった場合、サーバ担当者のセキュリティ意識向上のチャンスとして、指導に役立てています。

**Pros**

- 操作が監視されていることの認知
  自分のコマンド操作が常に監視されているということを認知させて、不正行為を抑止
- リスクのあるコマンドの認識
  どのようなコマンドがリスクがあるか認識し、リスクのある設定依頼などを未然防止

**Cons**

- 監視コスト
  監視に時間はかかるが、自動化が進んでいる（AccessCheckで集約できている）
- 確認頻度が高く、運用業務負荷
  頻繁にコマンド操作の確認があり、報告対応のため、業務負荷となる

**監視だけでなく抑止などの追加効果も視野に。**
**より意味のある監視にするために、定期的な改善を。**
**改善事例は次ページ**

# 事例②：操作ログの監視（改善例）

セキュリティ責任者とサーバ責任者がひざを突き合わせて改善方法を検討。

| | |
|---|---|
| **課題** | • セキュリティ担当からのコマンド操作への確認回数が多く、担当者は報告と調査、上司は、報告内容の確認で、**サーバ運用担当の負荷が増大** |
| **対策** | • 【セキュリティ】対象となるコマンドの精査<br>• 【サーバ】作業手順書の設置場所の共有<br>• 【サーバ・セキュリティ】確認方法、管理方法を改善<br>メールで都度確認→Teamsで、共同の管理表 |

**ポイント**

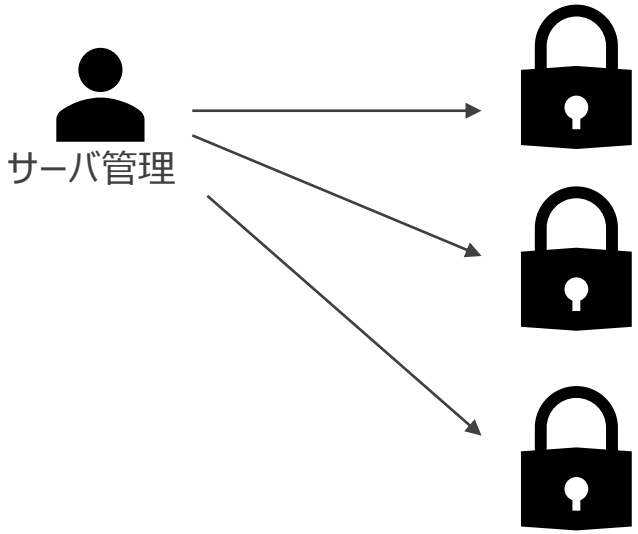
**①困っていることを声に出す**

**②会話して、お互いの業務への理解度を深める**

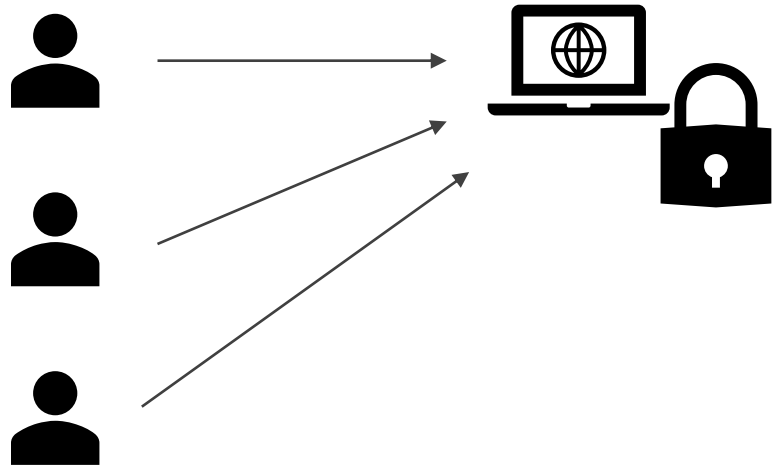
# 事例③：ID管理の一元化

サーバ担当者は多くのIDを個人で管理している状態だったので、一元管理し、他システムとの連携できる高機能なツールを導入しようとしたが、利用されない状態に。

**As-Is：各個人が管理**




**To-Be ：ツールで一元管理**



**個人管理の脆弱を改善しようとしたが、利用されない状態に**

# 事例③：ID管理の一元化（改善例）

ツールの導入は、利用者の巻き込みが必須。

| | |
|---|---|
| **課題** | • 管理するIDが多く、個人管理しているIDを移行するための時間の確保と運用変更が困難<br>• 高機能だが、すべての機能使うためには、構成変更・運用変更が必要 |
| **対策** | • 個人管理のIDの削減<br>サーバ毎に作成していた個人管理のユーザアカウントを廃止(AccessCheckの代理ログイン機能)<br>• ID管理に特化した低コストのツールに変更 |

**何を導入するのかではなく、どのように導入するかが重要。**
**代理ログイン機能に関しては、この後のセクションにて。**

# セキュリティ対策の効果を出すために

監視だけでなく抑止などの追加効果も視野に。
より意味のある監視にするために、**定期的な改善**を。

①困っていることを声に出す
②会話して、お互いの**業務への理解度を深める**

何を導入するのかではなく、**どのように導入するか**が重要。

# 「SecureCube Access Check」のさらなる活用

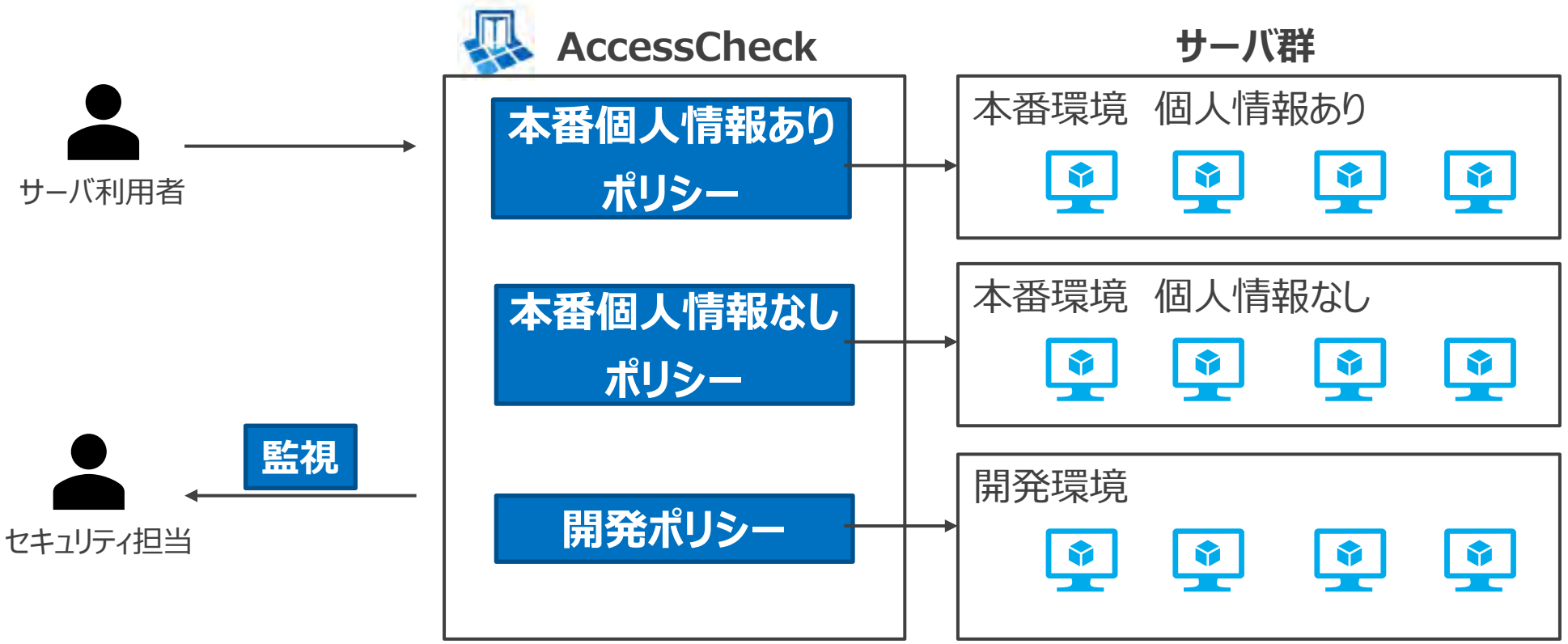
# 背景

きっかけは、AccessCheck v4のEOSL。
AccessCheckに関する業務は日々改善を行ってきたが、利用者増、サーバ増に伴い対応コストが高止まりしており、伐根的な対策が必要となっていた。

AccessCheckのリニューアルに伴い、セキュリティ向上と運用業務の改善を図った。

# AccessCheck v4 環境

AccessCheckの役割は大きく2点
- ポリシーで個人情報を隔離
- AccessCheckのログを監視

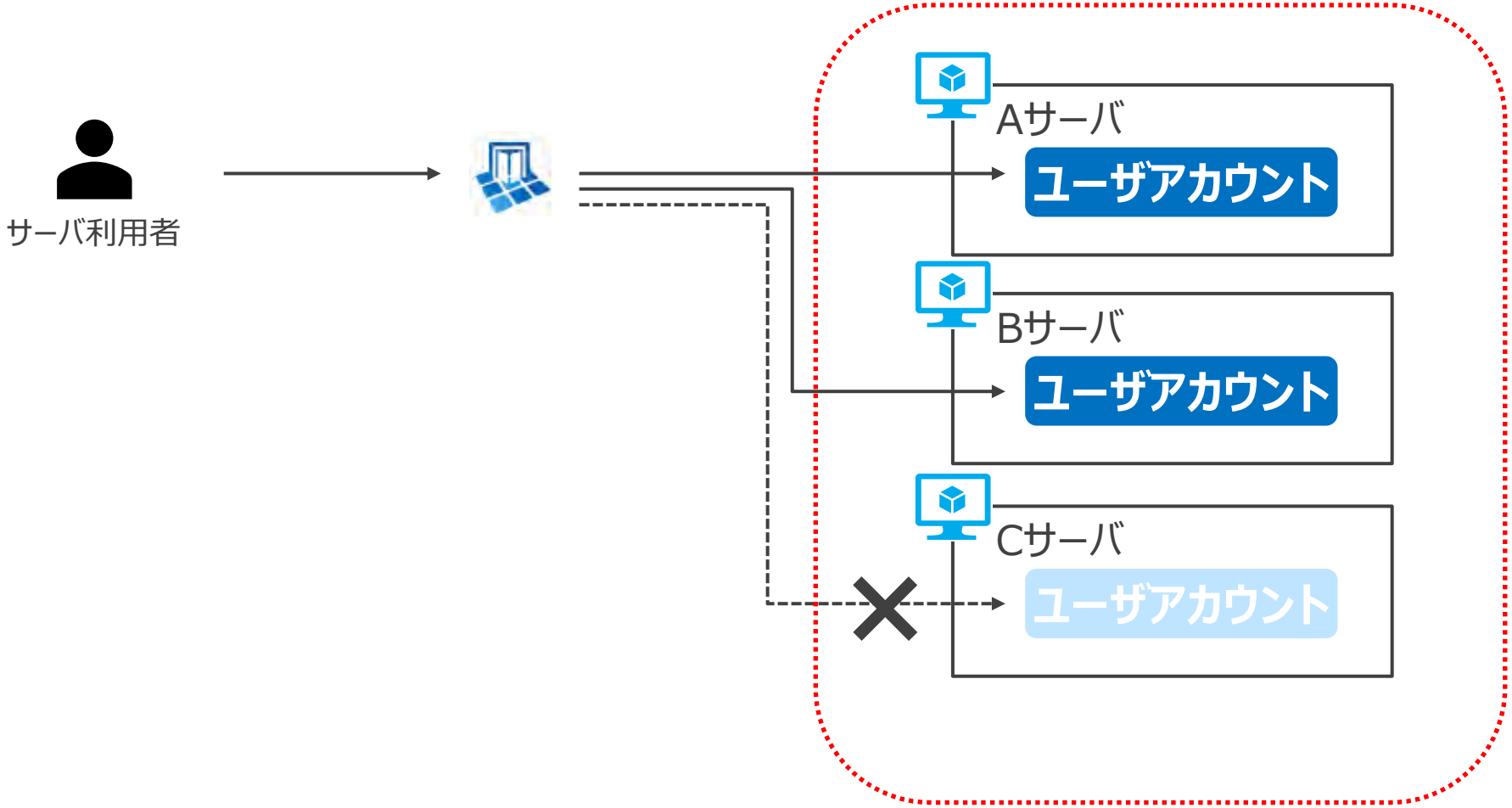


# 現行システムの課題

| | |
|---|---|
| **セキュリティ課題** | • アクセス権限制御はサーバ側であり、**全体の正確な把握に時間がかかる状態** |
| **運用課題** | • サーバ毎のアカウントで制御しているため、アカウント作成申請・アカウント棚卸の**業務が負荷**になっている |
| **利用者課題** | • 個人で数百のID/PWを管理し、**PW漏洩リスクやパスワード検索・入力の労力**が負荷となっている |

# セキュリティ課題

各サーバにサーバ利用者のユーザアカウントがあるかどうかで特権管理をしているため、どのサーバにアクセスできるかの把握は、全サーバのユーザアカウント状況を確認する必要がある



# 運用課題

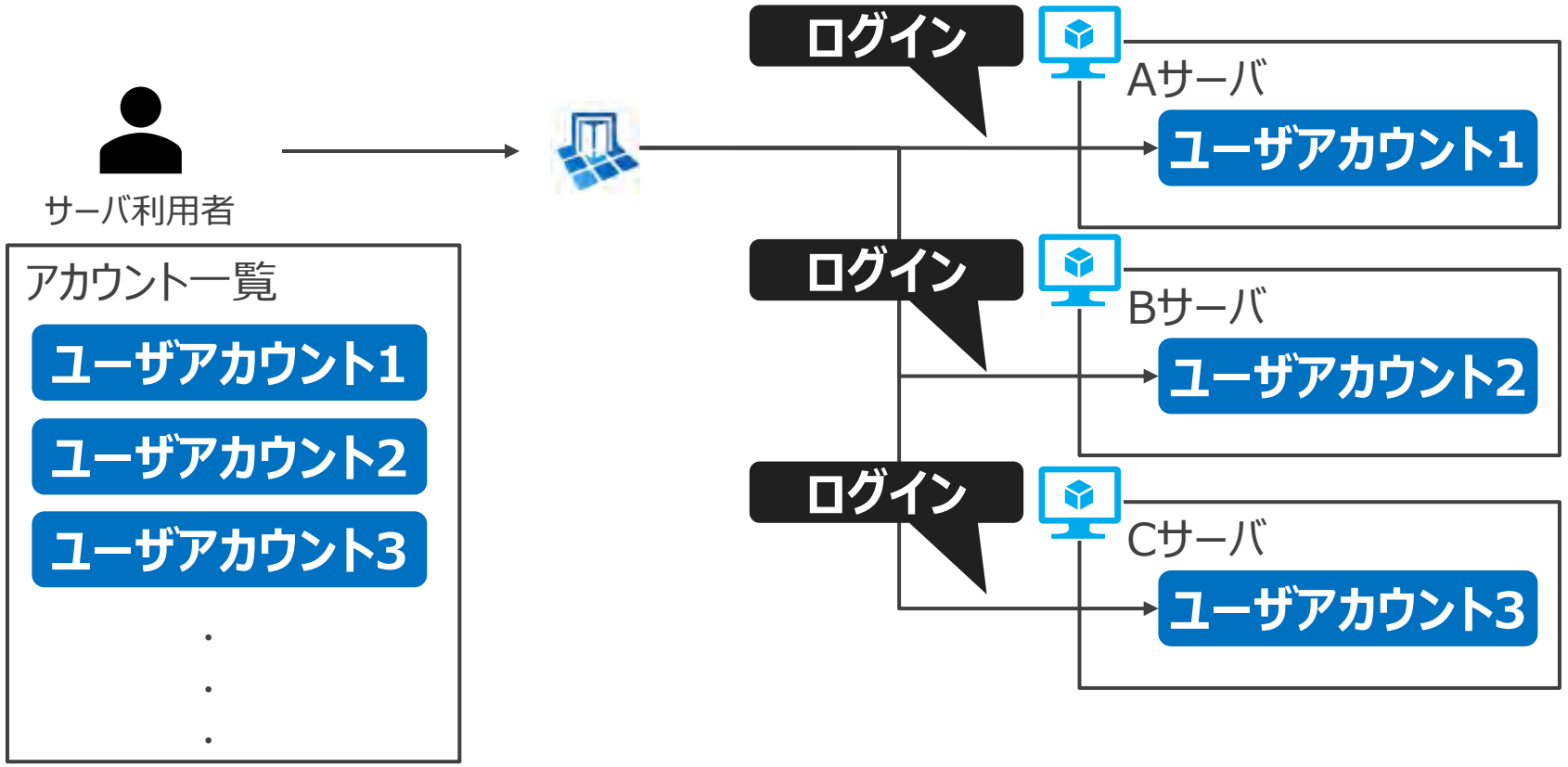
継続して改善を行っているが、運用工数で、年間約6,000時間かかっている。利用者増・サーバ増に伴い、さらに上昇し、運用工数が高止まりしている

運用工数

- サーバユーザアカウント作成・削除に関する工数：4,086時間/年
- AccessCheckアカウント作成・削除に関する工数：1,100時間/年
- サーバユーザアカウント、AccessCheckアカウント棚卸に関する工数：500時間/年

# 利用者課題

サーバ毎の個人のOSアカウントを管理し、接続時は、都度一覧を参照しログインを実施。担当者によって、数百のサーバを担当している。

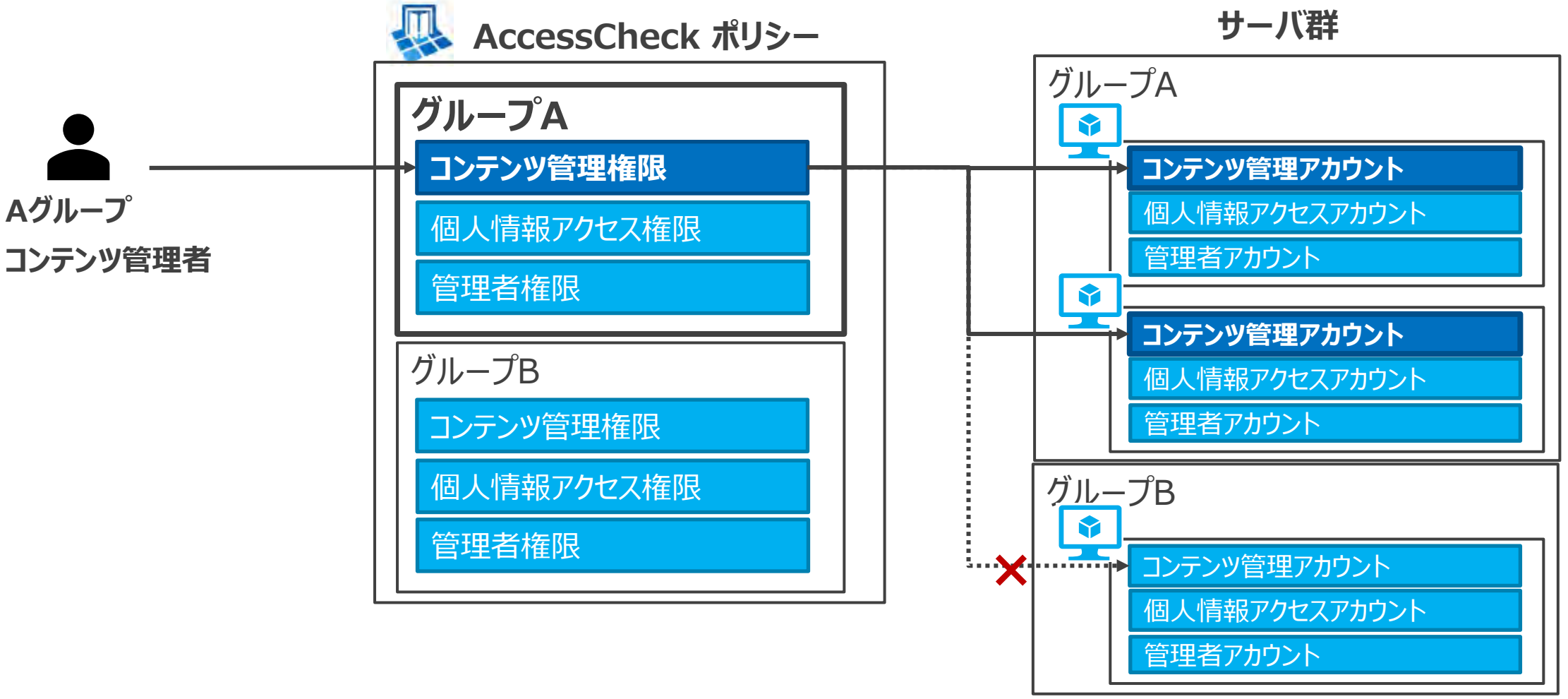


# 対策

| | |
|---|---|
| **ポリシー制御** | • AccessCheckのポリシーで一元管理することで、**統一ルールで、全体を把握**することが出来る |
| **代理ログイン活用** | • AccessCheck代理ログイン機能を利用して、サーバ毎の個人アカウントを廃止し、**アカウント管理による業務負荷軽減、PW漏洩リスク軽減** |
| **アクセス申請活用** | • **アクセス申請内容全体を可視化、公開** |

# AccessCheckポリシーで、一括制御

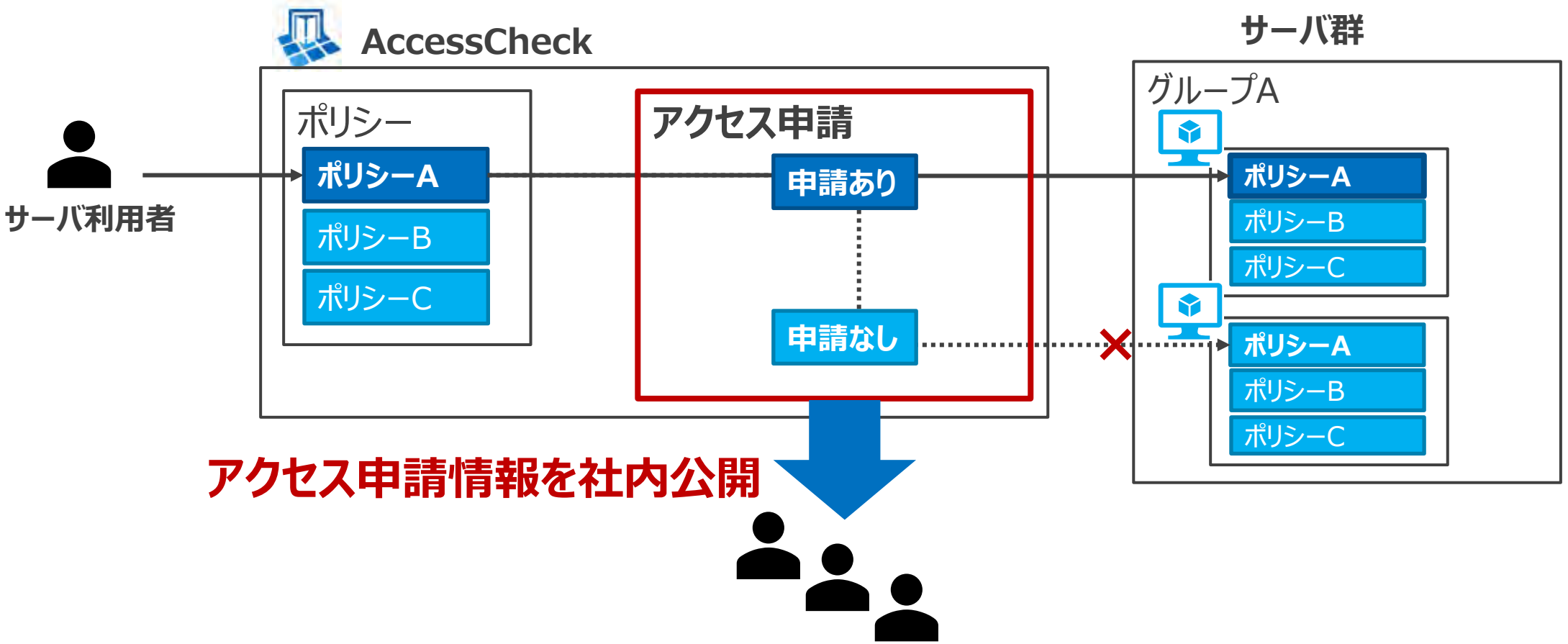
対象サーバのグループと利用者の役割に合わせたAccessCheckポリシーを作成し、一括で制御し、不要な役割やグループへの接続を制限。




**最も重要な設計となるので、現状運用状況と理想のギャップを明確にして、移行可能な計画を。**

# アクセス申請機能を利用して、接続状況の公開

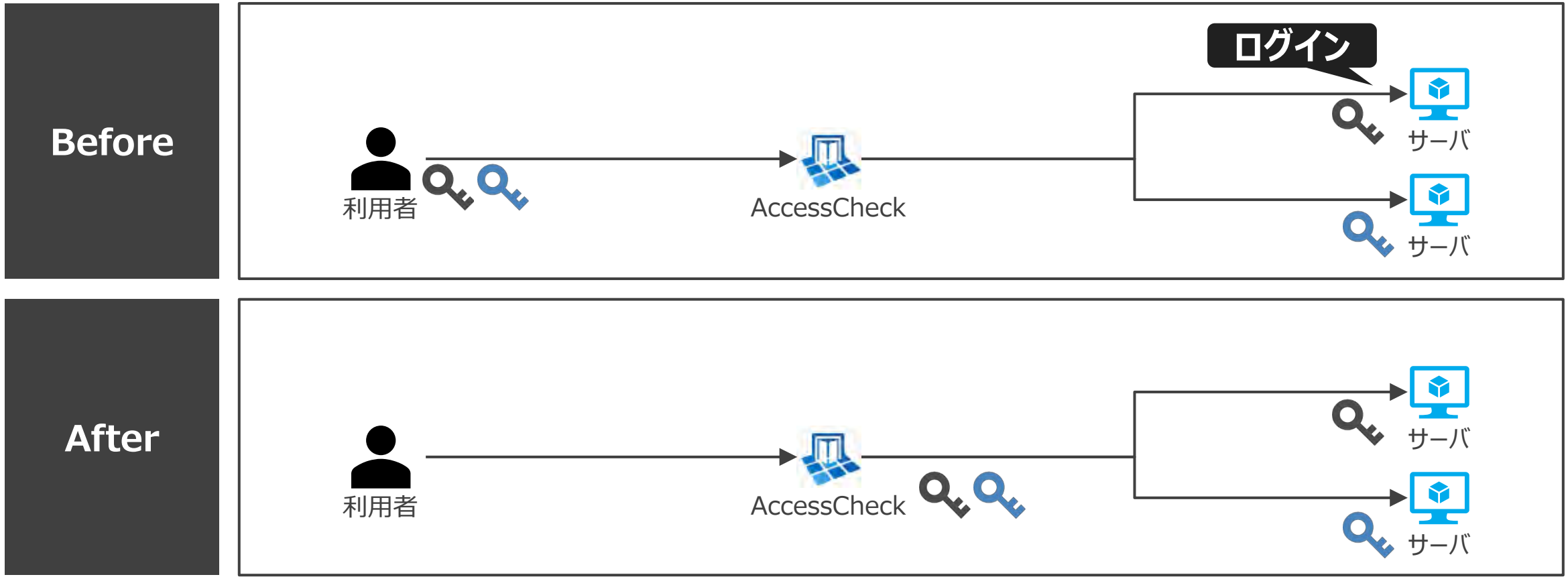
さらに、接続必要なサーバーのみ事前にアクセス申請し、接続可能な状態となる。
申請情報は社内公開し、全員の目で監視できる状態にすることで、心理的な抑止効果がある。




**利用方法は千差万別、各社に合った活用を。**

# 代理ログイン機能を活用して、ユーザアカウント管理の廃止

個人でそれぞれのサーバのユーザアカウントを管理していたが、AccessCheckで一括管理することで、個人の管理負荷が軽減




**運用効率に影響が大きい機能、導入検討を。**

# 利用者の声

サーバ管理　15年

大量のサーバのログイン情報を個人で管理していましたが、
管理不要となり**楽で安全**になりました。

サーバ毎のユーザーアカウントのパスワードを毎回、1台1台
確認して、ログインしていたのですが、ログインが楽になり、
業務**ストレスが軽減**されました！

サーバ管理　2年

サーバ管理　1年

サーバに接続するために、ユーザアカウントの作成を申請し、作
成されるまで数日待つ必要があったが、アクセス申請するとすぐに
利用できるようになり、**待ち時間が無くなり**ました。

# AccessCheck導入予定の方へ

AccessCheckから出力されるログの監視は有効。
利用者側へのフィードバックすることで、**最大限活用**できる運用もあります。

ポリシー、代理ログイン、アクセス申請など、多くの機能があるので、
**自社に合った設計**を初めにしっかり実施してください。

利用者側とセキュリティ側両方で、**お互いを理解**することで、
利用者の利便性とセキュリティを両立してください。

# End